



March 2, 2009

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, SW - Suite TW-A325
Washington, D.C. 20554

Re: **Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket No. 06-36**

Name of company
making this filing: NE Colorado Cellular, Inc.

Form 499 Filer ID: 809568

Name of signing officer: Michael Felicissimo

Title of signatory: Executive Vice-President

CERTIFICATION

I, Michael Felicissimo, hereby certify that I am an officer of the company(s) named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Customer Proprietary Network Information rules set forth in 47 C.F.R. §§ 64.2001 *et seq.* of the rules of the Federal Communications Commission.

Attached to this certification is an accompanying statement which (i) explains how the company's procedures ensure that the company is in compliance with the requirements set forth in 47 C.F.R. §§ 64.2001 *et seq.* of the Commission's rules, (ii) explains any action taken against data brokers during the past year, (iii) reports information known to the company regarding tactics pretexters may be using to attempt access to CPNI, and (iv) summarizes any customer complaints received in the past year concerning the unauthorized release of CPNI.

A handwritten signature in black ink, appearing to read "M. Felicissimo", is written over a horizontal line.

Name: Michael Felicissimo
Title: Executive Vice-President
Date: March 2, 2009

We are where you are.

STATEMENT

Carrier has established operating procedures that ensure compliance with the Federal Communication Commission ("Commission") regulations regarding the protection of customer proprietary network information ("CPNI").

- Carrier has adopted a manual and keeps it updated with FCC CPNI rule revisions, and has designated a CPNI compliance officer to oversee CPNI training and implementation.
- Carrier continually educates and trains its employees regarding the appropriate use of CPNI. Carrier has established disciplinary procedures should an employee violate the CPNI procedures established by Carrier.
- Carrier has implemented a system whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI.
- Carrier maintains a record of its and its affiliates' sales and marketing campaigns that use its customers' CPNI. Carrier also maintains a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign.
- Carrier has established a supervisory review process regarding compliance with the CPNI rules with respect to outbound marketing situations and maintains records of carrier compliance for a minimum period of one year. Specifically, Carrier's sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval regarding its CPNI, and a process ensures that opt-out elections are recorded and followed.
- Carrier has implemented procedures to properly authenticate customers prior to disclosing CPNI over the telephone, at Carrier's retail locations, electronically or otherwise. In connection with these procedures, Carrier has established a system of personal identification numbers (PINs), passwords and back-up authentication methods for all customer and accounts, in compliance with the requirements of applicable Commission rules.
- Carrier has established procedures to ensure that customers will be immediately notified of account changes including changes to passwords, back-up means of authentication for lost or forgotten passwords, or address of record.
- Carrier has established procedures to notify law enforcement and customer(s) of unauthorized disclosure of CPNI in accordance with FCC timelines.
- Carrier took the following actions against data brokers in 2008, including proceedings instituted or petitions filed by Carrier at a state commission, in the court system, or at the Federal Communications Commission: None.
- The following is information Carrier has with respect to the processes pretexters are using to attempt to access CPNI, and [if any] what steps carriers are taking to

protect CPNI: Employees are trained to be diligent with CPNI and assure identification.

- The following is a summary of all customer complaints received in 2008 regarding the unauthorized release of CPNI:

- Number of customer complaints Carrier received in 2008 related to unauthorized access to CPNI, or unauthorized disclosure of CPNI: 1
- Category of complaint:

1 Number of instances of improper access by employees

1 Number of instances of improper disclosure to individuals not authorized to receive the information

0 Number of instances of improper access to online information by individuals not authorized to view the information

0 Number of other instances of improper access or disclosure

- Summary of customer complaints received in 2008 concerning the unauthorized release of CPNI:

During 2008, a series of incidents occurred surrounding two separate, but related customer accounts. One of Viaero's customers was a possible homicide victim. A company employee with a personal connection to the victim's fiancée made unauthorized changes to the victim's Viaero account, changing the responsible party from the victim to the victim's fiancée. When this unauthorized access was discovered, the employee was questioned by supervisors, warned of the unauthorized nature of the access, and later terminated. This incident did not result in a customer complaint, but the company did detect the unauthorized access.

The victim's fiancée also complained to the company that he believed another Viaero employee was accessing his account detail and was providing that detail to members of the public, through verbal and online communication.. The company thoroughly investigated this claim, and did not find any evidence that the second employee had in fact accessed CPNI or engaged in any unauthorized disclosure of CPNI.